UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/715,643	11/17/2000	Yoav Raz	EMS-00201	8061

26339 7590 08/29/2006

MUIRHEAD AND SATURNELLI, LLC
200 FRIBERG PARKWAY, SUITE 1001
WESTBOROUGH, MA 01581

EXAMINER	
KIM, JUNG W	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 08/29/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/715,643	RAZ ET AL.	
	Examiner	Art Unit	
	Jung Kim	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 July 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7,13-16,18-20,22,26-30,36,39-47,49,50 and 52-60* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *26-30,36,39-47,49,50 and 54-60* is/are allowed.

6)☒ Claim(s) *1-7,13-16,18-20,22,52 and 53* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This Office action is in response to the amendment filed on July 3, 2006.

2. Claims 1-7, 13-16, 18-20, 22, 26-30, 36, 39-47, 49, 50 and 52-60 are pending.

Continued Examination Under 37 CFR 1.114

3. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 7/3/06 has been entered.

Response to Arguments

4. Applicant's arguments that the prior art of record does not teach the new limitations of amended claim 1, in particular the limitation of: detecting write operations of the storage device and performing, in accordance with detected write operations, virus scanning on those tracks to which write operations have been directed (Remarks, pg. 20) have been fully considered but they are not persuasive. From the teachings of the prior art of record, performing virus scanning when code is written to a storage device is an obvious step. As outlined below, Ko also provides an example, wherein virus scanning is performed on code that is received at a computing system wherein

macro operations within the code are analyzed for the presence of viral code. (col. 5:50-68) This feature ensures that code received at the computing system is immediately verified prior to initial processing of the code, which secures the code before the virus can be actuated. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to detect write operations to tracks of the storage device; and perform, in accordance with detected write conditions, virus scanning on those tracks to which write operations have been directed. One would be motivated to do so to detect unwanted code prior to actuating the unwanted code, Ko, ibid. Hence, claims 1 and 22 remain rejected under the prior art of record. Amended claims 36 and 47 claim inventions having detecting and performing means which define structure equivalent to those supported by the specification and hence are not anticipated nor rendered obvious by the prior art of record. Therefore, these claims are allowed.

Claim Rejections - 35 USC § 103

5. Claims 1-7, 13-16, 18-20, 22, 52 and 53 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wells U.S. Patent No. 6,338,141 (hereinafter Wells) in view of Frisch Essential System Administration (hereinafter Frisch), Kim "The Design and Implementation of Tripwire: A File System Integrity Checker" (hereinafter Kim) and Ko USPN 6,697,950. (hereinafter Ko)

6. As per claim 1, Wells discloses a method of detecting computer viruses on a single, stand-alone computer system or on a networked machine using an antivirus unit,

wherein a user of the antivirus unit designates a set of files on a system to be scanned (see Wells, abstract; col. 9:1-4). Wells does not expressly disclose providing a disk space having at least a portion that is partitioned into separate segments, each segment being accessed by at least one of a plurality of hosts, wherein a first one of the segments is accessed using a different file system than a second one of the segments. However, this configuration is found in networked operating systems. For example, Frisch teaches a UNIX operating system that enables a flexible partitioning capability wherein each partitioned segment is accessed using a different file system. (pgs. 409-414 'From Disks to Filesystems', especially pg. 409, first paragraph in the section) Moreover, Frisch discloses exporting local filesystems by a particular system for network access by other hosts to mount to their system. (pgs. 612-614 'Exporting Local Filesystems') Hence, it would be obvious to one of ordinary skill in the art at the time the invention was made for the method of detecting a virus to be actuated on a disk space having at least a portion that is partitioned into separate segments, each segment being accessed by at least one of a plurality of hosts, wherein a first one of the segments is accessed using a different file system than a second one of the segments, since it enables an administrator broader control to allow or restrict access to information on a disk by segmenting the disk on a partition level as taught by Frisch. (page 394, 2nd and 3rd paragraphs)

7. Further, Wells does not expressly disclose scanning for a virus on a portion of the disk that includes a part of the first and second segments. However, means of selectively checking the integrity of separate filesystems on a disk is a feature of the

UNIX tool Tripwire. Kim teaches how different filesystems on a disk can be checked by entering the paths of relevant filesystems as well as corresponding selection-masks, which classifies how to observe changes in the filesystem, in the Tripwire configuration file. (page 11, Figure 2 and related text) Furthermore, Kim teaches Tripwire as a function operating in a larger security methodology: the results of a Tripwire check can be used by a filter program. (page 12, 2nd paragraph, 'quiet option') It would be obvious to one of ordinary skill in the art at the time the invention was made to selectively scan separate filesystems on a disk space for viruses since it enables the method to secure any suspicious subset of data on a disk, even across partitions.

8. Moreover, the invention of Wells scans all types of files and does not limit scanning to only non-native files (Wells, 2:15-20); also file sharing between different operation systems is a common feature among networked systems. As taught by Frisch in a different chapter, non-native files are transferred between a UNIX system and any reachable system (non-local and/or non-UNIX) using commands "ftp" and "telnet". (pg. 587, 4th and 5th bullets) Non-native files downloaded from non-local or non-UNIX platforms are incorporated into the local filesystem, and likewise are a portion of the disk space to be scanned. It would be obvious to one of ordinary skill in the art at the time the invention was made for the antivirus unit, using a particular operating system, to access non-native files created using operating systems different from the particular operating system that is used by the antivirus unit in connection with scanning at least parts of the disk space for viruses since file sharing between platforms is a

common technique as known to one of ordinary skill in the art and as taught by Frisch, ibid.

9. In addition, Wells does not disclose the antivirus unit scans at least one of the segments without using file-based information of the particular operating system or of any host having access to the at least one segment. However, Ko discloses several techniques of scanning for viruses without using file-based information of the particular operating system or of any host having access to the at least one segment. Ko teaches it is common to use virus scanners to perform pattern matching on code to determine whether a known virus is present in the code, since this technique is simple and has a low false alarm rate. (col. 1:65-2:3) Ko also discloses a method and apparatus for detecting macro computer virus using static analysis, wherein macro operations within a document are located and compared to suspected macro operations against a profile, which enables detection of new macro computer viruses. (2:27-46) Neither of these techniques use file-based information to scan for viruses. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to combine the method of detecting a virus as taught by Ko with the method of scanning a filesystem to detect viruses as taught by Wells such that the antivirus scans without using file-based information of the particular operating system or of any host having access to the at least one segment. One would be motivated to do so since the technique of scanning by pattern matching is a simple but yet fail safe means of detecting known viruses, and the technique of detecting macro viruses using static analysis enables the detection of previously unknown viruses as taught by Ko, ibid.

10. Finally, Ko provides an example, wherein virus scanning is performed on code that is received at a computing system wherein macro operations within the code are analyzed for the presence of viral code. (col. 5:50-68) This feature ensures that code received at the computing system is immediately verified prior to initial processing by the computing system, which secures the code before the virus can be actuated. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to detect write operations to tracks of the storage device; and perform, in accordance with detected write conditions, virus scanning on those tracks to which write operations have been directed. One would be motivated to do so to detect unwanted code prior to actuating the unwanted code, Ko, ibid. The aforementioned cover the limitations of claim 1.

11. As per claim 2, the rejection of claim 1 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, the first and second segments correspond to different physical portions of the disk space. (Frisch, pg. 410, Figure 9-3)

12. As per claim 3, the rejection of claim 2 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, Frisch teaches an embodiment of the UNIX OS wherein the first and second segments overlap. (pgs. 39-41, "Links") It would be obvious to one of ordinary skill in the art at the time the invention was made for the first and second segments to overlap to enable information pertinent to multiple segments to be shared

between the segments as taught by Frisch, ibid. The aforementioned cover the limitations of claim 3.

13. As per claim 4, the rejection of claim 2 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, Frisch teaches an embodiment of the UNIX OS wherein the first and second segments do not overlap. (pg. 395, Figure 9-1, disk 1) It would be obvious to one of ordinary skill in the art at the time the invention was made for the first and second segments to not overlap to organize segments into distinct logical partitions as taught by Frisch. Ibid. The aforementioned cover the limitations of claim 4.

14. As per claim 5, the rejection of claim 1 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, Frisch teaches an embodiment of the UNIX OS wherein the first and second segments correspond to logical entities. (pg. 395, Figure 9-1, disk 1) It would be obvious to one of ordinary skill in the art at the time the invention was made for the first and second segment to correspond to logical entities since it enables a direct correlation between a physical partition and a logical partition as taught by Frisch, ibid. The aforementioned cover the limitations of claim 5.

15. As per claim 6, the rejection of claim 5 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, Frisch teaches an embodiment of the UNIX OS wherein the first and second segments overlap. (pgs. 39-41, "Links") It would be obvious to one of ordinary skill in the art at the time the invention was made for the first and second

segments to overlap to enable information pertinent to multiple segments to be shared between the segments as taught by Frisch, ibid. The aforementioned cover the limitations of claim 6.

16. As per claim 7, the rejection of claim 5 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, Frisch teaches an embodiment of the UNIX OS wherein the first and second segments do not overlap. (page 395, Figure 9-1, disk 1) It would be obvious to one of ordinary skill in the art at the time the invention was made for the first and second segments to not overlap to organize segments into distinct logical partitions as taught by Frisch, ibid. The aforementioned cover the limitations of claim 7.

17. As per claim 13, the rejection of claim 1 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, Kim teaches implementing at least part of Tripwire using stand-alone hardware. (Kim, page 12, section 4.3.1) It would be obvious to one of ordinary skill in the art at the time the invention was made to implement at least part of the antivirus unit using stand-alone hardware to ensure the inviolability of the integrity database used by Tripwire (Kim, page 12, section 4.3.1, first paragraph in the section, 2nd sentence) The aforementioned cover the limitations of claim 13.

18. As per claim 14, the rejection of claim 1 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, Frisch and Kim teach implementing at least part of the antivirus unit as a process running on at least one of the hosts (Frisch, page 43,

'Processes'; Kim, page 10, section 4.1.2, 'Scalability' and section 4.1.3, 'Configurability and flexibility'; Wells, col. 3, lines 10-11) It would be obvious to one of ordinary skill in the art at the time the invention was made for a part of the antivirus unit be a process running on at least one of the hosts since any application run on a machine comprises at least one process on the machine: as defined by Frisch, a process is a single program running in its own virtual address space. (page 43, last paragraph, first sentence) The aforementioned cover the limitations of claim 14.

19. As per claim 15, the rejection of claim 1 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, Frisch teaches the useable areas of a disk space are partitioned into separate segments in any given partitioned disk. (page 395, Figure 9-1, disk 1; page 410, Figure 9-3) It would be obvious to one of ordinary skill in the art at the time the invention was made for the useable areas of the disk space to be partitioned into separate segments to enable each disk partition to be usable to a user or application. The aforementioned cover the limitations of claim 15.

20. As per claim 16, the rejection of claim 1 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, Wells and Kim teach the antivirus unit scans useable areas of the disk space. (Kim, page 11, Figure 2; Wells, col. 1, lines 54-60) It would be obvious to one of ordinary skill in the art at the time the invention was made for the antivirus unit to scan useable areas of the disk space since these areas are workspaces having read/write privileges for users and applications and are prone to integrity attacks

when a virus attains these privileges. The aforementioned cover the limitations of claim 16.

21. As per claim 18, the rejection of claim 1 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, Frisch teaches an embodiment of the UNIX OS wherein a particular segment assigned to a first host is inaccessible to other hosts. (page 29, Table 2-3, 'no access'; page 30, 5th line 'Other Access' and Figure 2-1; pages 228-229 'Using Groups Effectively', especially page 228, 4th paragraph, second sentence) It would be obvious to one of ordinary skill in the art at the time the invention was made for a particular segment assigned to a first host to be inaccessible to other hosts for the purpose of enforcing non-use of those who do not require access to a segment. (Frisch, page 228, 4th paragraph, second sentence) The aforementioned cover the limitations of claim 18.

22. As per claim 19, the rejection of claim 18 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, Frisch teaches an embodiment of the UNIX OS wherein all of the segments are at least readable by the antivirus unit. (page 29, Table 2-3, 'read access only'; page 30, 3rd line 'Group access' and Figure 2-1; pages 228-229 'Using Groups Effectively', especially page 228, 3rd paragraph, first sentence and 4th paragraph, last sentence) It would be obvious to one of ordinary skill in the art at the time the invention was made for all of the segments to be readable by the antivirus unit to enable the antivirus unit to comprehensively check the integrity of the disk. (Frisch,

page 228, 3rd paragraph, first sentence and 4th paragraph) The aforementioned cover the limitations of claim 19.

23. As per claim 20, the rejection of claim 1 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, Kim and Frisch teach that at least a portion of the antivirus unit is provided on at least some controllers for disks corresponding to the disk space. (Kim, page 11, Figure 2, first entry '/etc' and Section 4.2; Frisch, pages 398-405, 'The Filesystem Configuration File', especially page 398, '/etc/fstab') It would be obvious to one of ordinary skill in the art at the time the invention was made for a portion of the antivirus unit to be provided on at least some controllers for disks corresponding to the disk space to enable a comprehensive integrity check methodology. The aforementioned cover the limitations of claim 20.

24. As per claim 22, the rejection of claims 1-8, 13-16 and 18-20 under 35 U.S.C. 103(a) is incorporated herein. (supra) In addition, Kim teaches a first scan at a first time and a second scan at a second time after the first time, wherein the results of the first scan are taken into consideration in the performing of the second scan as outlined in the invention covered in the claim 1-8, 13-16 and 18-20 rejections. (page 14, section 4.5) It would be obvious to one of ordinary skill in the art at the time the invention was made for there to be a first virus scan at a first time and a second virus scan at a second time after the first time and dependent on the results of the first scan since the scans are automated on a periodic basis and the integrity of the segments must be

accounted for consistent with preceding scans starting with the inception of the checks to ensure integrity is maintained over the course of multiple periods. (Kim, page 14, section 4.5, 1st paragraph of the section, 3rd sentence) The aforementioned cover the limitations of claims 22.

25. As per claims 52 and 53, the rejections of claim 1 under 35 USC 103(a) is incorporated herein. (supra) Neither Wells, nor Frisch, nor Kim, nor Ko disclose sharing access or restricting access to a segment with a first host when the antivirus unit is scanning the segment. However, it is notoriously well known in the art to choose between shared access or restricted access within a filesystem to promote singular access to those files where concurrent access is not desirable. For example, UNIX implements NT type file locks using Samba. Examiner takes Official Notice of this teaching. It would be obvious to one of ordinary skill in the art at the time the invention was made to share access or restrict access to a segment with a first host when the antivirus unit is scanning the segment. One would be motivated to do so as this provides the system flexibility to allow concurrent access to certain files for ease of access and restricted access to prevent concurrent changes as known to one of ordinary skill in the art.

Allowable Subject Matter

26. Claims 26-30, 36, 39-47, 49, 50 and 54-60 are allowed.

Communications Inquiry

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W. Kim whose telephone number is 571-272-3804. The examiner can normally be reached on M-F 9:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jung Kim
August 24, 2006

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100